CRITICAL ANALYSIS OF ANONYMOUS & MYSTERIOUS INTERPLAY BETWEEN I.T. AND TERRORISM FINANCING- A LEGAL PERSPECTIVE

By Mayura Manohar Sabne Advocate

1. INTRODUCTION-

The science of information technology was invented to aid the human civilization. Basically being the medium of communication, storage and transmission of data, it facilitated the complex activities of human life. It brought accuracy and precision in day to day activities of humans. Besides controlling physical and mental activities, it started influencing social and physiological sphere of humans. As I.T. has positive consequences, it couldn’t remain immune from criminal elements in society also. Thus, emerged the concept of cyberspace and along with that cybercrimes.

Terrorism, till date, is the most inhumane and deadliest crime on the globe. It also adapted itself to the I.T. revolution and started exploiting the hidden opportunities in cyberspace to fulfill its evil agendas. Terrorism is sustained and it thrives upon finances. Finances are the soul of it. The financing of terrorism is best described as octopus with tentacles spreading across vast territories as well as across a wide range of religious, social, economic and political realities¹. And, the I.T. revolution and digital age is the age of digital finances and economy. Thus, these two aspects interacted together very easily and they started a deadly relationship of mutual benefit.

In the light of this background, the present research makes an attempt to understand the conceptual development of term “information technology” and “terrorism financing”. In order to understand the finer points of the research topic, the Researcher has tried to take a concise overview of the various digital ways through which funds for terrorism are obtained and channel through which they are either placed and integrated into the financial system and then used or directly mobilized in the hands of terrorists.

After appreciating the basic concepts related with terrorism financing, the major consideration of the Researcher is twofold- to analyze the nexus between use of information technology and terrorism financing through cyberspace and the corresponding the Indian legal structure dealing with the offence of terrorism financing through cyberspace.

Thus, after going through all the above mentioned thorough exploration through legal lens, the Researcher has attempted to figure out the issues and challenges which this evil interaction poses before the Indian cyber law. This analysis has resulted into some concrete conclusions which are used by the Researcher to provide important practical recommendations.

¹Nimrod Rapheli, Financing of Terrorism: Sources, Methods and Channels, 15:4 Terrorism and Political Violence 59, 59 (2010), available at http://dx.doi.org/10.1080/09546550390449881, last seen on 17/06/2018
2. OBJECTIVES OF RESEARCH-

The present research is carried out with a view-
1) To understand the concept of information technology and terrorism financing and study its nexus;
2) To critically evaluate the Indian legal provisions dealing with suppression of terrorism financing through cyberspace;
3) To provide practical recommendations for converting failures into successes;

3. RESEARCH METHODOLOGY-

The present research is doctrinal research. It employs descriptive, analytical, evaluative and interactive legal research models. The present paper has utilized primary data available from various statute books and secondary data which are available from various books written by authors of international and national acclaim, various online journals available on the website of jstor, oxford and online resources of websites of Finance Ministry of India etc. The Researcher has used SILC Rules for citation methodology.

4. ANALYSIS-

A) CONCEPTUAL DEVELOPMENT OF TERM “INFORMATION TECHNOLOGY” AND “TERRORISM FINANCING”–

The term information technology is defined as “the technology involving the development, maintenance and use of computers and software for the processing and distribution of information.” It is science which basically deals with information which in simple terms known as “data”. This data can be of any type—social, economic, financial, political etc. Thus, the science of information technology pervades into every sphere of human life. The history of development of information technology is not very old; however, it has evolved with such a fast pace that today, every human being on the globe is living in two worlds—one is the real or physical and another is the virtual world which is commonly known as “cyberspace”. Therefore, all the traditional human activities, benevolent as well as maleficent, which are carried on in the real world are now taking place in cyber space. And terrorism is no exception to it.

The World Bank and International Monetary Fund have defined financing of terrorism as “the financial support, in any form, of terrorism or of those who encourage, plan or engage in it.” The fund raising methods of wide range of groups are most often lumped together under the general rubric of terrorism financing.

Terrorism financing is generally understood as an activity which deals with collecting and accumulating funds in order to sustain terrorism or donating to the terrorist organizations or networks, sometimes with complete knowledge regarding the intentions of the receiver of

---

2 Information Technology, available at https://www.merriam-webster.com/dictionary/information%20technology, last seen on 30/06/2018

3 Thomas J. Biersteker & Sue E. Eckert, The Challenge of Terrorist Financing, 1, 6 in Countering the Financing of Terrorism (Thomas J. Biersteker & Sue E. Eckert, 2008)

the funds and sometimes with complete ignorance about the misuse of funds.

Thus, it can be seen that terrorism financing covers within its purview all those activities which provide funding to terrorist activities of individual terrorists or lone wolf fighters, terrorist organizations and networks. The terrorist activities include operation, training, propaganda, recruitment, compensation, social support mechanisms in one form or another. Therefore, it can be said that terrorism financing is the heart and driving force behind any terrorist activity.

B] NEXUS BETWEEN INFORMATION TECHNOLOGY AND TERRORISM FINANCING-

After having understood the basic concepts of information technology and terrorism financing, it is important to look through the nexus between these two.

The sources of terrorism financing can be categorized according to the activities and persons or entities involved in it.

Following are the types of sources-

Thus, it can be seen that cyberspace is one of the main invisible players which contributes as source of terrorism financing.
Cyber space aids terrorists in the following ways-

Money generated through above mentioned sources assumes significance only when it is channeled safely through suitable path to reach its objective. Following are the various channels engaged by terrorists to move their funds and all these channels are now a days rampantly being exploited by terrorists through cyber space-

All the above depicts that in today’s digital age, information technology and terrorism financing are in beneficial mutual relationship. This interaction was evident in the year 1997, when Babar Ahmad, A British citizen from South London, through Azzam Publications and Associated websites, supporting Afghanistan-Taliban and Mujahedeen in Chechnya, incited donors under the garb of religious obligations and solicited funds for the cause of jihad. This is merely a drop in the ocean, if we consider the omnipotent presence of cyber space as of today. All the major terrorists’ organization in the world like Al-Qaeda, Hamas, Laskher-e-Toiba, Hezbollah and ISIS, throughout their operations, at all stages and levels use cyberspace for fulfilling their funding needs.

---

5 Michel Jacobson, Terrorist Financing on the Internet, 2(6), CTC SENTINEL, 17,17(2009) available at www.supremoamicus.org
Starting with basic function of creating propaganda and soliciting funds through simple online methods, the terrorists have adapted themselves to the most modern and advance cyber technology employed through smartphones like m and e money, internet banking, wire transfers, use of cryptocurrency for financing themselves. This mutual relationship has thrived through decades due to following reasons-

1. Cyber space masks the identity of terrorists so that they can easily use their hidden identity for spreading propaganda and attracting recruits.
2. The borderless reach of cyber space aids in training of terrorists recruits throughout globe.
3. The widest reach of cyber space in the nook and corner of globe presents infinite points for generation of funds.
4. Cyber space offers anonymity which facilitates storage of funds.
5. The speed and ease offered by cyberspace aid transfer of funds.
6. The dissolution of geographical barriers achieved by cyber space expedites the mobilization of terror money in the shortest possible time without being easily detected by the counter terrorism financing agencies.
7. The lack of privacy in cyber space offers terrorists enormous pool of data for exploitation which is utilized for committing financial cybercrimes and securing funds for their terrorist activities.
8. The transnational nature of cyber activity amplifies the potential impact of terrorism on the victim.

Thus, the Information technology through enormous veiled opportunities is assisting terrorism financing through all the above mentioned facets. At the same time, in order to harness the hidden potential of cyber space, terrorist intelligentsia is, through inventions of new technological advances, contributing towards the evolution of information technology. This mutual exchange has become the deadliest intersection of two superpowers and is posing serious challenge before the international and Indian cyber law and in front of the counter terrorism financing agencies also.

The existence of this reciprocal relationship is universal and omnipotent and hence India is also one of the major victims of this evil collaboration.

LEGAL FRAMEWORK - AT INTERNATIONAL & REGIONAL LEVELS –

The global digital community has shared the fruits of cyber technology in unanimity. Simultaneously, the absence of geographical boundaries in cyber space helped the cyber terrorists to carry out terrorism financing through multiple jurisdictions at one and the same time. This phenomenon made the various nations the victims of cyber terrorism financing and therefore, a need was felt to take stringent legal action against this cybercrime of terrorism financing through cyberspace.
Unfortunately, the global community is divided on the definition of “terrorism” itself and hence, it has failed to formulate a universal legal binding instrument specifically addressing the all-pervasive facet of cyber terrorism financing. Under the guidance of Security Council resolution bearing number 1373 of 2001 pertaining to terrorism financing, terrorism financing is made a criminal offence. Further, the Security Council Resolution number 2253 of 2015 condemned the use of modern information and communication technology by terrorists and urged the member states to take measures of identifying, listing and suppressing the activities of financing terrorism through cyberspace. However, it must be noted that these are mere resolutions and they lack effective enforcement force.

Apart from this, at regional level, there are following legal instruments which deal with cybercrime of terrorism financing:

a. The Council of Europe Convention on Cybercrime, 2000;

These legal instruments do not deal exclusively with terrorism financing but they substantially cover all those cybercrimes like data theft, hacking, phishing, credit and debit card frauds etc. which are included in financing activities of terrorists through cyberspace. Apart from these regional arrangements, The United Kingdom has pioneered in framing a national legislation to counter the use of internet for terrorist purposes.

2] INDIAN CYBER LAW DEALING WITH CYBER TERROR FINANCING -

a. Legislations

India has always contributed significantly in the development of international law dealing with combating terrorism and for countering it’s financing. India is signatory to The International Convention for the Suppression of the Financing of Terrorism, 2001. India has keenly and progressively implementing the Security Council Resolutions also.

India is the architect of the Comprehensive Convention on International Terrorism which has been submitted to United Nations in the year 1996 and is still under consultation in the UN Committee. After the terrorist attacks anywhere in the world, India has made an appeal to the international community to set aside their differences on various issues arising out of interpretation of the Convention and adopt the Convention collectively.


7The Use of Internet for Terrorist Purposes, Report by UNDOC and CTITF, available at https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, last seen on 30/06/2018

www.supremoamicus.org
In regional context, it has been found that India is one of the active members of ASEAN, SAARC and BRICS. India is committed to accord regional co-operation with full strength and vigor on these multiple fore in the fight against terrorism financing.

The offence of terrorism financing is criminalized in India, pursuant to various International Conventions and Resolutions. Indian statues dealing with the crime of terrorism contains provisions which are aimed at curbing menace of terrorism financing and they are as follows-

a. The Unlawful Activities Prevention Act;
c. The Foreign Exchange Management Act [FEMA], 1999;
d. The Prevention of Money Laundering Act, 2002 (Amended Up to Date);
e. The Foreign Contribution (Regulation) Act, 2010 [FCRA]

Apart from these counter-terrorism legislations, the Indian cyber law has been laid down in the form of The Information Technology Act, 2000. Initially when the Act was enacted in the year 2000, it did not contain any provision for prevention of cyber terrorism. The reason behind this was that India was not that much technologically advanced nation at that time and the information technology revolution in India was also at nascent stage. However, with the strong influence of globalization, the information technology developed in India by leaps and bounds for the period of next six to seven years. The U.S. war on terror post 9/11 and the global efforts to curb terrorism financing through cyber space had positive impact on Indian legal fraternity. Simultaneously, India also felt a need of law to curb the growing menace of cybercrimes. In the light of all these developments, The Information Technology Act was amended in the year 2008 which incorporated new provisions dealing with cyber terrorism and national cyber security 8. However, the scrutiny of newly added provisions reveals that it nowhere includes the offence of terrorism financing committed through electronic medium.

The misuse of digital or crypto currency for raising funds is imminent threat to Indian financial security. However, current Indian Information Technology Act has still not taken this warning into consideration. Moreover, the terrorist organizations are m ole sting opportunities on the internet and social media platforms for spreading their malevolent propaganda and ideology and for radicalizing Indian youth. In spite of having knowledge of this widespread exploitation, the said Act still has not incorporated provisions for punishing hate speech made by terrorist leaders using these cyber platforms.

b. Executive Initiatives-

Apart from formulating and enforcing the Information Technology Act, 2000 (Amended up to date), India has also framed the National Cyber Security Policy in the year 2013. The Cyber Security Policy aims at protection of information
infrastructure in cyberspace, reduce vulnerabilities, build capabilities to prevent and respond to cyber threats and minimize damage from cyber incidents through a combination of institutional structures, people, process, technology and cooperation. The objective of this policy in broad terms is to create a secure cyberspace ecosystem and strengthen the regulatory framework. The policy addresses various issues like public-private partnership, collective engagements through technical and operational co-operation, research and development in cyber security, development of human resources through education and training programs and national awareness programs.

However, the critical review of the said policy reveals that in the backdrop of such speedy development of information technology in India, the policy has not been reviewed once since its birth. Though it tries to cover multiple aspects of strengthening cyber security framework in India, the dream envisaged is inadequate considering the emerging trends in cybercrime. Further, by not taking into consideration the significant development like cloud computing, the Policy proves to be insufficient for laying down strong cyber security framework. The policy creates multiple offices responsible for cyber security at various places but fails to define their exact jurisdiction and hence, it suffers from ambiguity and conflict of interest is the inevitable result of this vagueness.

Along with the above policy, National Crisis Management Plan for countering cyber-attacks and cyber terrorism has been prepared and is being updated annually. Central Govt. Ministries or Departments and States and UTs as well as organizations in critical sectors are making efforts to prepare and implement their own sectorial Crisis Management Plans. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats or vulnerabilities and countermeasures to protect computers or servers on regular basis. It conducts regular training programs for key stakeholders. The critical analysis of these initiatives points out towards a grim fact that it nowhere deals with the crime of terrorism financing through cyberspace. The growing terrorist attacks and revelation of transnational terror funding links through cyber space demands effective and stringent Executive Policies and actions. In the wake of recent initiatives of demonetization policy and digital India Campaign, it is imperative of the day that the Executive must provide secure cyber environment for effective digital cashless transactions. However, that


11PTI, Saving Cyber Network from Criminal Treat, Press Information Bureau, Government of India (07/03/2018) available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=177079, last seen on 30/06/2018
view of cyber security is nowhere reflected in all these enterprises. All these initiatives look attractive on paper but up to what extent they have been successfully implemented in reality is the most important question which is nowhere answered by any Department or Ministry of the Indian Government.

**C. Role of RBI and SEBI**

Terrorism financing is financial crime and therefore, the financial guardians like the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) are also charged with the responsibility to devise counter terrorism financing measures in order to protect stability and integrity of Indian financial system.

The boom in the usage of crypto currency and transfer of money through such virtual currency was initially not paid heed to by RBI. RBI merely issued warning in respect of use of virtual currencies including bit coins. However, the surge in such usage and the demand of global market security currents have forced RBI to think upon the said issue seriously and in view of the associated risks, RBI decided that, with immediate effect, entities regulated by RBI shall not deal with or provide services to any individual or business entities dealing with or settling VCs. Regulated entities which already provide such services shall exit the relationship within a specified time. This circular has positive intention but RBI has failed to provide any grievance redressal mechanism for bona fide investors. As it is recently issued, its impact can be judged only over a long period of time.

The Securities and Exchange Board of India, another regulator of Indian financial market has also issued a statement that the regulations on crypto currencies should be out soon. In the light of lightening developments in the usage of cryptocurrencies and their vulnerability for terrorism financing makes it mandatory that the Guidelines and Rules must implemented with effective force and vigor.

**5. Issues and Challenges**

The detailed analysis from the critical point of view of the nexus between information technology and terrorism financing through cyberspace reveals that the information technology and its beneficial avenues are aiding terrorists in their funding. At the same time terrorists are facilitating growth and development as well as spread of information technology revolution. The international and national legal systems, being aware of this evil co-operation, have made an attempt to criminalize terrorism financing through cyberspace but their actions are interrupted due to following issues –

**1. Multiple Jurisdictions**

---

12) PTI, Use of Bitcoin, other virtual currencies not authorized by RBI, says govt., The Hindu(28/03/2017), available at www.thehindu.com/business/Economy/use-of-bitcoin-illegal-says-govt/article17702483.ece, last seen on 30/06/2018
14) Rules on Crypto Currencies should be out soon: SEBI Chief, PTI available at https://www.livemint.com/Money/VmmuGPeknFAlQsjoN0YzDK/Rules-on-cryptocurrencies-should-be-out-soon-Sebi-chief.html, last seen on 30/06/2018
The borderless nature of commission of crime of terrorism financing through cyber space gives birth to the issue of jurisdiction as the crime is capable of being committed in multiple jurisdiction at one and the same time. When the terrorists sense that they are insecure in one jurisdiction, they commit the cybercrime and immediately, they relocate their operations to other jurisdiction where there is absence or inadequacy of law dealing with the same cybercrime. The international criminal justice system, unfortunately, does not have a universal legal instrument which is the answer for this issue of multiple jurisdictions. Neither there is uniformity and consistency throughout multiple national legal systems with respect to punishing cybercrimes. The national criminal justice systems are diverse in nature and they are bereft of cooperation. This hampers effective investigation as it becomes difficult to secure electronic evidence from such multiple jurisdictions.

2. Anonymity-
The mysterious nature of cyberspace offers anonymity to terrorists and hence they can easily generate, store and mobilize funds. Anonymity also provides them some security as it is very difficult to keep surveillance of cyber space for all the time. The tool of encryption is further aiding the terrorists in masking their identity and hence, they can mobilize funds with ease without being detected by the counter-terrorism financing agencies. Thus, the issue of anonymity and security provided to it is one of the significant issues.

3. Dynamic nature of Digital data and electronic evidence-
In order to carry out effective investigations into the crime of terrorism financing through cyber space, it is imperative to construct money trail. To trace the source of digital terror funding, the investigators have to collect digital data and electronic evidence from multiple jurisdictions. Most of the times, they have to recover the destroyed data. While doing all this, they have to encounter the human rights issues related to surveillance and interception. They also have to secure electronic evidence stored on multiple electronic devises which are various components of information technology. They have to preserve the digital data in appropriate manner because it has very fragile nature. They also have to answer the questions related to the originality and authentication of such evidence before the prosecution agencies. All these requirements are serious issues before the investigation as well as law enforcement agencies.

4. Lack of Cyber Jurisprudence-
The act of terrorism financing has been made an offence at international as well as national levels. However, the national legal systems do not deal with the crime of terrorism financing through cyber space as an exclusive offence. All the arena of cybercrimes which come under the purview of financial cybercrimes and which directly or indirectly, aid terrorists in garnishing funds are punished. Thus, the lack of exclusive offence of terrorism financing through cyber space hampers the effective prosecution of terrorism financing. Further, even if it is accepted...
fact that all the traditional financial crimes are committed in cyber space in the same manner, they do have some differential characteristics. These differences need separate treatment and hence, the lack of cyber jurisprudence poses an important issue.

5. Failure of Traditional Criminal Justice-
As already pointed out by the researcher, the legal architecture dealing with the crime of terrorism financing through cyber space is riddled with several lacunas. The Executive initiatives are also haphazardly drafted and poorly implemented. Along with these foundational deficiencies, the Indian criminal justice system responsible for prosecution and for punishing the said crime, itself suffers from its own inherent limitations of delay and latches. It lacks that pace of adaptation which is exhibited by the information technology revolution. The lack of technical capabilities and expertise to investigate the cybercrimes and the inadequacy of infrastructural faculties further proves to be obstacles in effective prosecution of the cybercrimes. The multiple enforcement and investigative agencies, the competition and rivalry among them and conflict of jurisdictions of multiple regulators obstruct the already weak criminal justice system. Thus, the poor legal foundation along with unsatisfactory criminal justice system is serious issue which needs immediate attention.

6. Infringement of Fundamental Rights-
While investigating the crime of terrorism financing through cyber space, sometimes investigators are required to have access to confidential financial and personal data possesses by trade entities. This interference adversely affects the fundamental right of carrying on trade. Another fundamental right which is liable to be breached during investigations and prosecution of the said crime is the right to privacy. Though nothing remains private once it enters into virtual space, the inherent and indestructible right to privacy must be safeguarded in cyber space also. Use of legitimate ways under legitimate circumstances can only protect these two fundamental rights. Only when there is unlawful or arbitrary access, disclosure or use of confidential information is evident, the investigation agency should interfere with the enjoyment of these fundamental rights. Thus, securing balance between the legitimate requirements of the investigation and prosecution of crime of terrorism financing through cyberspace and secure enjoyment of fundamental rights of to freedom of trade and to privacy creates another significant issue in this present context.

All the above discussed issues pose array of challenges to be tackled with by the international as well as national legal fraternity-
1. Tracking and monitoring digital financial systems to construct online money trail while safeguarding right to freedom of trade and right to privacy;
2. Formulating universal legal instrument targeting terrorism financing through cyber space;
3. Implementing regional agreements and models laws which has universal application and uniform common standards accepted across multiple jurisdictions;
4. Securing electronic evidence through multiple jurisdictions and preserving its originality and authenticity;
5. Developing uniform and consistent rules of cyber jurisprudence;
6. Updating and adapting law as per the dynamic demands of the information technology revolution;
7. Encountering anonymous and secure nature of cyber space;
8. Infusing new vigor, vitality and force into the slow moving and weak Indian criminal justice system by immunizing it from delay and latches;
9. Building adequate and sufficient infrastructural facilities along with empowerment of human resource to produce technical expertise.

Apart from abovementioned particular challenges, considering the change in nature of terrorist organizations from organizations to network, from hierarchy to horizontal connections, it can be seen that the financing needs have undergone significant changes. Earlier hierarchical and large terrorist organizations required large amount of funds on consistent basis and the sources and channels of funding were limited, constrained by geographical boundaries and under greater vigilance of counter terrorism financing agencies. Whereas today individual terrorists and terrorist networks require less amount of funds that can be easily available through multiple sources and channels available through cyber space. This linked transformation has posed significant challenge before the Counter terrorism financing agencies because earlier it was easy to construct to money trail in physical world and to collect the evidence for prosecution. But today virtual nature of funding through cyber space hardly leaves any traces to be tracked and thus speed challenges investigation.

Another dilemma with respect to the same challenge is that whether to allow the trail to be continued over cyber space so that original source can be traced and destroyed or to interrupt the trail at intermediate stage to prevent its future occurrence and punish immediate perpetrators. This dilemma is the major challenge before the investigation agencies because each option presents its own pros and cons and it depends whether the counter terrorism financing policy seeks to achieve long term goals or short term results.

6. CONCLUSION AND RECOMMENDATIONS
   The pace of information technology revolution is enormous and with its rapid development, it is posing unknown dynamic challenges before law. The terrorist intelligentsia is exploring these covert avenues and securing finances for their growth and sustenance. This mutual co-existence and collaboration is creating grave issues before the international as well as national legal systems and before the counter terrorism financing agencies. These issues are challenging the capabilities of these institutions and demands their adaptation and transformation as per the changing needs and times.

   The law must adapt itself to the pace of revolution and keep itself all inclusive and updated. Law must see through psychological and social foundations of the crime of terrorism financing. It must assess
the psychological and social reasons which support and sustain the terrorism by aiding and facilitating the funding of terrorism through cyberspace. Along with preventive and punitive approach, law must also provide for advocacy initiatives.

The global cyber law community must offer an integrated and coherent response and accept a common accord respecting all the diverse features and characteristics of numerous national criminal justice systems. The developed nations must work hand in hand with developing and under developed nations. They must support these technologically backward nations with efficient financial support, training and access to advanced technological infrastructure. The international legal fraternity must lay down architecture for various national legal systems to follow so that they can build and develop a strong and uniform cyber security infrastructure.

Along with contributing to the international efforts, states must also adopt positive attitude towards international legal developments. They must refrain from supporting any kind of terrorist activity. They must insulate their jurisdictions and shared cyber space from being abused by terrorists for their financing purposes. With due respect to human and fundamental rights, the states must provide stringent cyber security mechanism with effective and balanced surveillance. The said mechanism must possess effective counter terrorism financing internal compliance system empowered with adequate infrastructural faculties and capable human resources and expertise.

The challenges presented by this evil interface should be converted into opportunities to prevent and suppress the crime of terrorism financing through cyberspace. The same cyber avenues must be used to gather intelligence in advance. The infinite data must be analyzed smartly to secure sufficient electronic evidence. The online money trail must be utilized to reach the original source so that the crime can be nipped in the bud itself.

In specific Indian context, India is also the victim of above discussed issues and challenges and hence the researcher recommends that it is high time now that India must shed its political biases and become a signatory to the European Convention against Cybercrime. It will facilitate the Indian access to international legal framework working for cyber security. India is marching towards digital economy and virtual society. In the light of this development, India is continuously reviewing its cyber law but it’s very slow moving. It lags behind the speed of information technology revolution. It is need of the hour that India must make amendments to the existing cyber law so it can effectively address all the issues and challenges posed by terrorism financing through cyber space. In general context, India lacks comprehensive counter terrorism financing policy. India must formulate such policy which shall encompass all economic, criminal, financial, political, and social and cyber facets of countering financing of terrorism. The said policy, inter alia, shall provide for –
a. criminalization of terrorism financing over the internet or other cyber related services;
b. enlargement of investigative powers of counter terrorism financing agencies;
c. regulation of internet related financial services;
d. Human rights protection and adherence to the rule of law principles.

The said umbrella policy shall also provide for consolidated legislation which shall target exclusively and independently all the angles of terrorism financing from all inclusive preventive and curative perspectives. As a special requirement, it shall develop specialized judicial and evidentiary procedures for prosecuting cyber offences related to terrorism financing. India must follow the suit of European Union, Australia, Indonesia which has developed effective cyber security mechanisms targeted at preventing the spread of emerging cyber terrorism financing threats such as misuse of crypto currencies.

Last but not least, as crime emerges from the society, the community participation in detection and prevention of crime is sine qua non for suppressing any crime. The global cyber community consisting of billion users and million stakeholders shall shoulder the responsibility along with the legislative and executive machinery to prevent the occurrence, growth, spread and development of the cybercrime of terrorism financing. The public-private partnership is the best solution to suppress the crime and harness the beneficent potential of information technology revolution.

*****